For : The Patent Application Our Ref. :NT0226US

- LIST OF THE PRIOR ART REFERENCES CITED IN THE SPECIFICATION

1. Advances in Cryptology-CRYPTO etc.

2. The Chain & Sum Primitive and Its Applications to MACs And Stream Ciphers
Mariusz H. Jakubowski and Ramarathnam Venkatesan
(281-293)
"Advances in Cryptology CRYPTO'98" Kaisa Nyberg(Ed.)

3. Keying Hash Functions for Message Authentication
Mihir Bellare and Ran Canetti and Hugo Krawçzyk (1-328)
"Advances in Cryptology CRYPTO'96" Neal Koblitz (Ed.)

4. An Integrity Check Value Algorithm for Stream Ciphers
Richard Taylor (40-48)
"Advances in Cryptology CRYPTO'93" Douglas R.Stinson (Ed.)

5. Algorithm Types and Modes (189-401)

6. UMAC: Fast and Secure Message Authentication
J.Black, S.Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway
(pg.216-269)
"Advances in Cryptology CRYPTO'99" Michael Wiener (Ed.)

7. MMH: Software Message Authentication in the Gbit/Second Rates Shai Halevi and Hugo Krawczyk (172-189)
"Fast Software Encryption" Eli Biham (Ed.)

8. Integrity-Aware PCBC Encryption Schemes
   Virgil D Gligor, Pompiliu Donescu (1-13)
"The 1999 Security Protocols Workshop Pre-proceedings"

9. Stream ciphers based on LFSRs (203-369)

Reference				
Richard Taylor	An Integrity Check Value Algorithm for Stream	pp.40-48	LNCS773	CRYPTO93
Mihir Bellare Ran Canetti Hugo Krawczyk	Keying Hash Functions for Message Authentication	pp.1-15		CRYPTO96
M. Atici D. R. Stinson	Universal Hashing and Multiple Authenitcation	pp.16-30	LNCS1109	CRYPTO96
Tor Helleseth Thomas Johansson	Universal Hash Functions from Exponential Sums over Finite Fields and	pp.31-44	LNCS1109	CRYPTO96
Victor Shoup	On Fast and Provably Secure Message Authentication Based on	pp.313-328	LNCS1109	CRYPTO96
Mariusz H. Jakubowski Ramarathnam Venkatesan	The Chain & Sum Primitive and Its Applications to MACs and Stream Ciphers	pp.281-293	LNCS1403	EUROCRYPT98
J Black S. Halevi H. Krawczyk T. Krovetz P. Rogaway	UMAC: Fast and Secure Message Authentication	pp.216-233	LNCS1666	CRYPTO99
Mark Etzel Sarvar Patel Zulfikar Ramzan	Square Hash: Fast Message Authentication via Optimized Universal Hash	pp.234-251	LNCS1666	CRYPTO99
Jee Hea An Mihir Bellare	Constructing VIL-MACs from FIL-MACs: Message Authentication under Weakened Assumptions	pp.252-269	LNCS1666	CRYPTO99
Shai Halevi Hugo Krawczyk	MMH: Software Message Authentication in the Gbit/Second Rates	pp.172-189	LNCS1267	FSE97
Virgil D. Gligor Pompiliu Donescu	Integrity-Aware PCBC Encryption Schemes		The 1999 Security Protocols Workshop Pre-proceedings, Cambridge UK, 1999.	
Alfred J. Menezes Paul C. van Oorschot Scott A. Vanstone	Handbook of Applied Cryptography	pp.203-212, 250-259, 263-266, 347-349, 352-	ISBN0-8493-8523-7	
Bruce Schneier	Applied Cryptography, second edition	pp.189-209, 398-	ISBN0-471-11709-9	

The excerpt from the relevant Notice of reason for rejection

- related claim: 1
- references: No. 1 and No. 2

Following are the descriptions "the encrypted message authentication using a chaining technique" (p. 103-109) in reference No. 1 discloses.

"One of the methods for applying the authentication mechanism is to utilize the error propagation characteristics gained from using a chaining technique. This concept can be explained for reference purposes with respect to a block chaining method using both plaintext and ciphertext for feedback (Fig. 2-16). This technique has an advantage that both security and authentication can be achieved in one operation."

"Suppose that X(1), X(2),..., X(n) are the plaintext blocks encrypted by a key K and an initialized vector Z, and that Y(1), Y(2),...,Y(n) are ciphertext blocks obtained as a result."

"Note that an additional plaintext block X(n+1) is attached to the end of the text to allow a computation Y(n+1)=AC to be performed. As one example, the additional block equals the initialized vector as a definition. As other approaches, the additional block may have a specified constant value, for example, all zero bits, or may use the first block X(1) repeatedly."

"By judging if X(n+1) is equal to Z, it can be decided whether the recipient accepts or rejects the message (Fig. 2-38). The receiving side accepts the message if X(n+1) is equal to Z, because only the sending side who knows the secret key K must first create Y(n+1) correctly. The message is rejected in other cases." (p. 104-105)

Taking the description above, Fig. 2-38 and Fig. 2-16 into consideration, reference No. 1 is summarized as follows.

"A symmetric -key encryption method comprising the steps of:

dividing plaintext composed of redundancy data and a message to generate a plurality of plaintext blocks each having a predetermined length;

outputting a feedback value obtained as a result of operation on the plaintext block and the ciphertext block that is an encrypted block of the plaintext block concerned, said feedback value being fed back to another plaintext block; and

performing an encryption operation using the plaintext block, a secret key and the feedback value obtained as a result of operation on another plaintext block to produce a ciphertext block."

The present invention concerning claim 1 "generates a random number sequence based on a secret key; generates a random number block corresponding to one of said plurality of plaintext blocks from said random number sequence"; and uses the generated "random number blocks" for both a feedback value operation and an encryption operation for ciphertext blocks. Reference No. 1, on the other hand, does not generate random number blocks, but uses the ciphertext blocks for a feedback value operation, and uses a fixed secret key for an encryption operation for ciphertext blocks.

There are the following descriptions in reference No. 2:

"This paper proposes a model which allows the concealment of plaintext as well as an authentication based on an information theoretical approach, showing an implemented example" (p.1 "abstract").

"This paper argues about how a message authentication is important, in particular in a field of communications, proposing a technique for enabling a message authentication along with an encryption operation."

"This research shows an approach that enables a message authentication by using pseudo random number sequence the size larger than a message length with a redundancy added by a fixed length, in a stream cipher field using pseudo random numbers in encryption operation."

"A major target in this research lie in optimizing a throughput of both plaintext and ciphertext. For this purpose, the proposed method performs the calculation of cipher elements as independent of a plaintext and a ciphertext as possible. This approach is similar to dividing a block cipher operation into a key scheduling part and a data scrambling part. That is, it is similar to considering a problem of how constructing a stronger key scheduling part can make a data scrambling part simpler, when designing a block cipher mechanism." (p. 1-2 "1 introduction)

"In this section, symbols + and × denote addition and multiplication, respectively, in the general finite field, while -**a** and $\mathbf{a}^{-1}$ about an element **a** denote the inverse elements in addition and multiplication, respectively.

Theorem 2 Suppose that **F** is a finite field with the elements as many as q. Suppose that the number of elements in plaintext set **P**, ciphertext set **C**, and addition key set **A** is q, respectively; the number of elements in multiplication key set **A** is q-1. Suppose that the element of a certain plaintext, ciphertext, addition key or multiplication key embedded into the finite field is **p**, **c**, **a** or **b** ($\neq 0$), respectively. When **a** and **b** are given uniformly and at random, a cryptosystem where the ciphertext **c** is determined as follows proves safe information-theoretically in both concealment and completeness."

"$\mathbf{c}=(\mathbf{a}\times\mathbf{p})+\mathbf{b}$

proof: [concealment] With $\mathbf{a}\neq 0$, a mapping f: $\mathbf{p}\rightarrow\mathbf{a}\times\mathbf{p}$ is a bijection. **b**, which is selected uniformly and at random, is regarded as a encrypted key thrown away after one use, and this cryptography possesses information-theoretically safe concealment".

This characteristic is also implemented in terms of a cryptosystem defined by **c=(a+p)×b**" (p. 3-4 "4 implemented model and safety"

"Our model finds the safety by computational complexity —non-linearity— not in a data scrambling part, but makes a pseudo random number generation independent of others, making the data scrambling part dedicated to scrambling.

Here, it is convenient to consider a multiplication on the finite field as an ideal function for the purpose of scrambling. Concealment is maintained by adding random numbers while the change after alteration becomes not anticipated by multiplication. This technique guarantees that the change of ciphertext against different plaintexts grows uniform on the condition that the random numbers are thrown away after use.

These techniques enable building the specific examples of cipher processing, characterized by a processing method using both the operations on a finite field and the pseudo random number sequence the size truly longer than that of the plaintext, as shown above." (p. 6 "5.3 frequent key update and the design of block cipher)

In summary, reference No. 2 describes the following: in order to simultaneously carry out both an encryption for concealment and message authentication, the technique utilizes the random numbers longer than the plaintext as addition keys and multiplication keys; and it encrypts a plaintext having a redundancy by adding and multiplying the plaintext and the keys on a finite field, with at least the addition keys thrown away after one use.

The inventions described in reference No. 1 and No. 2 have a feature of simultaneously carrying out both encryption and message authentication in common. It is obvious to one of ordinary skill in the art to apply the invention described in reference No. 2 to the invention described in reference No. 1 in such a manner that the ciphertext block operations use random number blocks each thrown away after use --that is, those corresponding to plaintext blocks— generated by pseudo random number generator, instead of fixed secret keys. Note that it is obvious to ordinary skill that the pseudo random number generator generates the random number sequence by use of a secret key.

In addition, considering that a ciphertext is a kind of pseudo random number, there is hardly any particular difficulty in that the invention described in reference No.1 uses random number blocks generated from random number sequence, instead of the ciphertext blocks, for the feedback value operations although the present invention uses plaintext blocks and random number blocks for those operations.

Accordingly, the present invention concerning claim 1 is what ordinary skill would have been able to come around to that thinking, based on the inventions described in references No. 1 and No. 2.